AtGuard Getting Started Guide

Welcome to AtGuard

AtGuard blocks annoying ads and cookies and puts a personal firewall on your PC. AtGuard delivers:

- Increased performance-AtGuard dramatically speeds the downloading of web pages. AtGuard blocks banner ads and reduces download time. In addition, AtGuard keeps animated images on web pages from repeatedly displaying the animation sequence, further reducing clutter.
- Improved privacy-You can block cookies that allow a site to track data about you and your web use.
- Greater protection-Use the personal firewall feature to decide who gets access to your PC, and when. You can also block your PC from connecting to specific sites or making a certain type of connection. Restrict access by IP address, network port, time period, or by application-and enjoy peace of mind.

Installing AtGuard Software

AtGuard runs on Windows 95, Windows 98, Windows 2000, and Windows NT 4.0 with Service Pack 3 or higher. You must have the Microsoft TCP/IP network protocol installed on your machine to run the AtGuard software.

AtGuard installation involves two basic steps:

1. Download the compressed version of the AtGuard Setup program.
2. Once you download this file, run it to automatically decompress the Setup file and install AtGuard.

After restarting your PC, you're ready to put AtGuard to work for you.

After You Install

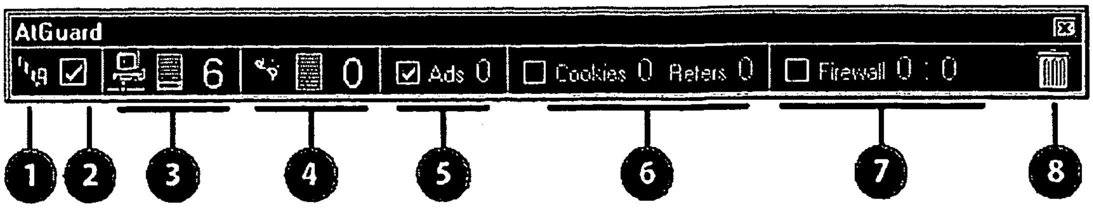
When AtGuard is running, the AtGuard dashboard is on your desktop and the AtGuard icon is on the Windows taskbar.

- On a Windows NT or Windows 2000 machine, and on many networked machines, the AtGuard icon is on the taskbar when you start Windows.
- On a Windows 95 or Windows 98 machine, AtGuard might not start right away. If you use dial-up networking to connect to the Internet, you may need to dial before you see the AtGuard icon and dashboard.

You can always start AtGuard by using the Start menu. Click the Windows Start button, point to Programs, point to AtGuard, and then click Start AtGuard.

Using the AtGuard Dashboard

The AtGuard dashboard makes a variety of AtGuard functions readily available on your desktop. Using the dashboard, you can monitor your web and network activity and see how much work the ad blocker, the privacy filters, and firewall are doing for you.



❶ Click the dashboard menu to get to other AtGuard utilities and settings, to reset the counters, and to paste images into the Ad Trashcan.

You can change the way the dashboard looks. Click Properties to select which parts of the dashboard should be displayed on your desktop.

❷ The main AtGuard check box starts or stops AtGuard filters for ads, cookies and other privacy settings, and the firewall.

❸ The network activity gauge and the counter next to it show all the current network connections going in and out of your machine. Click on the counter to see details about these connections.

❹ The web activity gauge and the counter next to it show the web activity on your machine. As you move between web pages in your browser, this number changes.

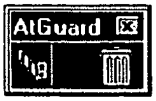
❺ The Ad Blocker check box enables and disables ad blocking. The **Ads** counter shows how many ads have been blocked as you surf the web.

❻ The Privacy Protection check box enables and disables a filter that blocks cookies and refer fields. The **Cookies** counter increases as cookies are blocked, and the **Refers** counter increases when refer fields are blocked.

❼ The Firewall check box enables and disables the firewall. When you enable the firewall filter, firewall rules control which connections you allow to and from your PC. The **Firewall** counters tell you how many times your firewall rules have permitted or blocked a network connection.

❽ Paste an image from a web page to the Ad Blocking Trashcan so that you won't have to see it again.

Changing the Look of the Dashboard



You can move the dashboard anywhere on your desktop, and you can resize it so that only the Trashcan and the menu are visible.

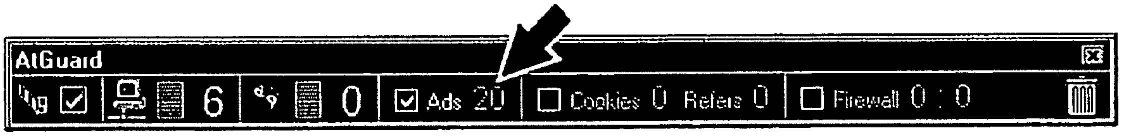
Using the AtGuard Icon on the System Taskbar

The AtGuard icon is on the system taskbar notification area (usually in the right corner at the bottom of the screen).

Click the AtGuard icon to get to AtGuard utilities and settings, disable AtGuard filters, or exit AtGuard (remove it from computer memory). There's also a menu option to let you hide the dashboard and then turn it back on when you want to use it.

How to Tell if AtGuard Is Working

1. Use your web browser to connect to a web site, then do a bit of web surfing to other web pages.
2. Look at the AtGuard dashboard. Has the number next to the Ads counter increased?



If the number is anything other than zero, AtGuard is working.

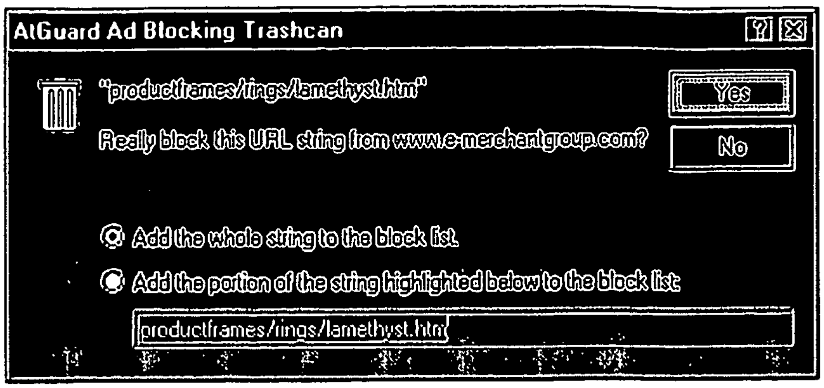
If the counter does not change, then AtGuard is probably not configured correctly to monitor web activity. You may have a proxy server causing the problem. Look up "proxy" in the online help to find out how to resolve this problem.

Using the Ad Trashcan

AtGuard blocks many ads on web pages without any effort from you. However, you may see ads or images that you'd like AtGuard to block. The Ad Trashcan, located on the right end of the AtGuard dashboard, provides a quick way to "throw away" an image or ad and prevent it from being displayed in the future.

To block an image or ad by putting it in the Ad Trashcan:

1. Right-click an image or ad.
   - In Internet Explorer 3.0 or 4.0, click Copy on the shortcut menu.
   - In Netscape, click Copy Image Location on the shortcut menu.
   - In any other browser, copy the HTML string that provides the link location to the Clipboard. If your browser allows you to right-click an image and copy the image location to the Clipboard, you should be able to paste it onto the Ad Trashcan.
2. Right-click the Ad Trashcan on the dashboard. On the shortcut menu, click Paste Into Trashcan.
3. AtGuard will figure out the correct URL (Uniform Resource Locator, the web address) for the image and show a confirmation dialog box that looks like this:



AtGuard Ad Blocking Trashcan

"productframes/rings/amethyst.htm"

Really block this URL string from www.e-merchantgroup.com?

○ Add the whole string to the block list.

● Add the portion of the string highlighted below to the block list:

productframes/rings/amethyst.htm

If you click Yes, the image will be blocked whenever you load that page again.

To block more than one image at a time:

When you see a URL string in the confirmation dialog box, you can highlight a portion of it to block more than one particular image. For example, highlighting everything except "amethyst.htm" in the example above will block all images and ads from the "rings" folder on the e-merchantgroup.com site. Be sure to pick the option to "Add the portion of the string highlighted below..." before you click Yes.

Beyond the Basics

After you have used AtGuard for blocking ads, you'll be ready to learn more about how AtGuard works and what else AtGuard can do.

How AtGuard Blocks Ads and Images

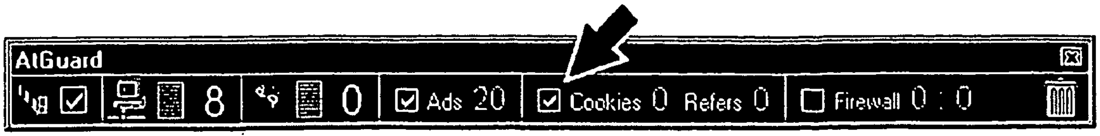
Web pages are be made up of special tags to incorporate all of the text, images, windows that display other web pages, and even audio or video clips into their pages. Some of these tags tell the browser to connect to a specific server and request a particular file. A page that has an excessive number of these requests, such as one with several different advertisements, can slow down the loading of a web page dramatically.

When you request a web page in your browser, AtGuard compares its list of sites and graphics that should be blocked with any tags that might request them. If one of these requests is on a web page, AtGuard removes it from the page before the page is displayed by the web browser.

Since the AtGuard Ad Blocker keeps the image from ever being requested, pages load faster.

Protecting Privacy by Blocking Cookies and Refer Fields

To start using cookie blocking, select the Privacy Protection check box on the dashboard (next to the **Cookies** and **Refers** counters). By default, this also turns on the CookieAssistant, which will help you create a cookie rule when one is required.



☑ 8 0 ☑ Ads 20 ☑ Cookies 0 Refers 0 □ Firewall 0 : 0

What Are Cookies?

Cookies are bits of information that web servers store on your computer for their later use. Web sites can use cookies to keep track of how many times you've visited and what sort of information you've been looking for on their site. They can even use cookies to pass that information on to other web servers that manage advertisements.

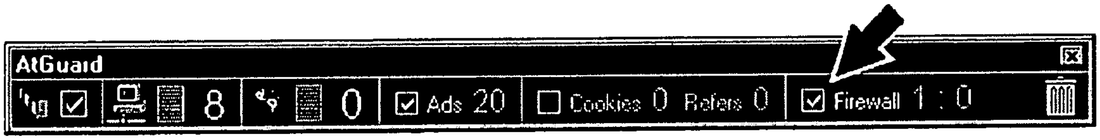
You may not want to block all cookies. For example, an online shopping site may use cookies to remember items placed in your "shopping cart" at an online shopping site. AtGuard lets you decide which cookies to permit.

What Are Refer Fields?

Refer fields allow web servers that you visit to know where you've just been. You may prefer to keep this information to yourself. AtGuard's privacy protection also lets you block refer fields.

Controlling Access with the AtGuard Firewall

To enable the firewall, select the Firewall check box on the dashboard.



☑ 8 0 ☑ Ads 20 □ Cookies 0 Refers 0 ☑ Firewall 1 : 0

The next time you connect to the Internet, you'll see the AtGuard RuleAssistant. The RuleAssistant will guide you through options to permit or block communication. If you wish, you can make a rule so that the firewall knows how to handle the same connection type in the future.

AtGuard's firewall gives you control over network communication coming in and going out of your computer. The firewall can:

- control who connects to your computer and who your computer can connect to.
- keep data from being transmitted without your knowledge.
- warn you about attempts to use resources on your computer that you might otherwise not know about.
- help you learn about the resources your computer makes available to others on the Internet.

Getting More Information

There are a variety of product support and information resources:

- **AtGuard Product Online Help**

The AtGuard product online help provides a lot of information about setting up and using AtGuard. This is the first place to look when you need assistance. Right-click the AtGuard icon or click in the dashboard menu, then click Help. You can also click the Help button in AtGuard dialog boxes. Right-click an area in a dialog box and then click What's This? to see a short explanation of a specific item.

Home |

The unofficial @Guard FAQ

July 30th, 1998

Written by Aaron Logue and Mary Rayborn,
with much help from the @Guard people!
Comments/updates to atfaq@cryogenius.com

----- 1. INTRODUCTION -----

1-1. About this FAQ

This FAQ is intended to provide more information about @Guard to newcomers and seasoned users alike. Herein you will find basic info about @Guard and how it works, how to make it do what you want (or make it stop doing what you don't want), how to suggest features to the people working on it, and where to get updates, blocklists, and more information.

This FAQ is available at http://www.cryogenius.com/atguard
You can find additional information at http://www.atguard.com

1-2. How to contribute to this FAQ

If you have something you'd like to add to this FAQ, please send email to atfaq@cryogenius.com. It will be reviewed, and if accepted, added to the FAQ.

Please note that all submissions to the FAQ become the property of the authors and that they may or may not be acknowledged. By submitting to the FAQ, you grant permission for use of your submission in any future publications of the FAQ in any media. The authors reserve the right to edit any submission in any manner necessary, or omit it entirely.

1-3. Acknowledgements

First off, I'd like to thank WRQ, without whom all this wouldn't have been possible. The folks at WRQ have been known for quietly producing high quality corporate software for years, but have recently come "out of the box" with this very cool performance enhancement and firewall package for mainstream internet users.

1-4. The FAQ doesn't answer my question. What do I do?

If your problem isn't mission-critical, you can send an email to the FAQ at atfaq@cryogenius.com and wait for it to get answered here.

You can also send an email to nam-feedback@technologypreview.com and check their FAQ for updates. That email address can also be used to ask the developers about things, but they're pretty busy folks so you may or may not get a reply.

----- 2. THE BASICS -----

2-1. What is @Guard?

@Guard (pronounced "At Guard") is a Windows kernel device driver that you install on your PC that monitors network traffic going in and out of your computer. Specifically, it can:

- o Prevent software from communicating with your computer or with remote computers without your knowledge (has an interactive learn mode where it pops up dialogs asking you what it should do until it's got your wishes figured out)
- o Block images (usually advertisements) that you don't want to see
- o Speed up web page loading (try www.javaworld.com w/ and w/out the blocker)
- o Block refer fields and cookies to reduce the amount of targeted advertising you receive
- o Let you customize web pages that you visit often
- o Keep track of various statistics as you surf, like how much data you've downloaded and how many cookies you would have sent
- o Stop distracting animated GIFs from cycling endlessly
- o Stop some JavaScript popups, like those things on Geocities and Tripod pages

2-2. Who wrote it?

The biggest software company you never heard of, WRQ in Seattle, WA. They're something like the 16th largest PC software company in the world and have a web page at http://www.wrq.com.

2-3. Where can I get it?

You can find atguard.exe at http://www.atguard.com, or more specifically, right at http://wrqdownload.wrq.com/techprev/atguard.exe

2-4. How much does it cost?

No price has been set yet. What's available right now is a "Technology Preview" that times out 30 days after it's installed. The best rumor I could get my hands on was that it'll probably wind up somewhere around $30, depending on interest level and feedback. By the time you read this, a pointer to a buydirect.com or software.com site should be available at the www.atguard.com page.

2-5. For which operating systems is it available?

Windows 95 or greater and Windows NT 4.0, Service pack 3. Alas, it is not available for Macintosh, but for image and cookie filtering I can recommend WebFree, available at http://www.falken.net/webfree/

Note: @Guard will NOT run on any 3rd party TCP/IP stack, including WRQ's own. @Guard hooks the TDI interface in Microsoft's stack.

2-6. I just installed it. What do I do now?

Start surfing! Depending on where you go, a whole bunch of ads should now be gone, your car will run smoother, your food will taste better, and the web will be a happier place.

You should have a little icon of a yellow and black striped gate on the right side of the taskbar. Click on it and a menu will appear. Try them!

"Statistics" Brings up a window with various counters on it Note that you can clear these by right-clicking in the window.

"Ad Trashcan" Brings up a little window with a trashcan that you can paste image and link URLs (Netscape) or drop link URLs (Explorer) into to add stuff to the blocklist.

"Event Log" Brings up a log of all sorts of interesting things, including a record of images blocked and which blocklist entry caused the blocking to occur, a list of past connections to remote computers, a list of cookies and refer fields and what happened to them, a history of URLs that have been visited, and a log of connections that were denied by the firewall.

"Settings" Brings up the configuration dialog, where you can turn various blocking features on and off, add strings to the blocklist, add individual domains to allow cookies to, modify firewall rules, and password protect @Guard's settings.

"Help" Brings up a most excellent online help. Most of your questions can probably be answered here.

2-7. How do I uninstall it?

In the unlikely event that you want to uninstall it, :) you can go to "Add/Remove Programs" in the Win95 or WinNT control panel, select "@Guard", and hit the Add/Remove button.

Beware that uninstalling really uninstalls; any blocklist and firewall rule set entries that you created WILL BE LOST. Hopefully, they'll have a way to save and restore the blocklist and rule sets before too long.

2-8. How do I tell if I have the Microsoft TCP/IP stack installed?

Win95 and NT come with the Microsoft TCP/IP stack, so this usually isn't a problem. If you go to My Computer->Control Panel->Network (then go to the "Protocols" tab if you're using NT) you should see something like "TCP/IP Protocol".

Newer versions of @Guard (2.0 build 6 and later) check for the Microsoft

TCP/IP stack at install time and refuse to install if it isn't found. Older versions of @Guard did the same, but only on Win95.

WRQ has also created a standalone utility to do a quick check, available at http://www.atguard.com/stackcheck.html

----- 3. Blocking Graphic Images -----

3-1. How do browsers load graphics and how does @Guard block them?

When you go to a web page, your browser might receive something like this:

```
  Blah! Blah blah: <img src="http://www.foo.com/nifty_images/image7.gif">
```

When your browser sees that, it prints the text "Blah! Blah blah:" on the screen, and then it connects to www.foo.com and asks it for a file called "/nifty_images/image7.gif". If www.foo.com has such a file, it sends it to the browser, which displays the image.

This same mechanism is used to gather up all the different pieces that can make up a web page, including images, windows that display other web pages (also known as frames), and even audio or video clips.

So a single web page can be constructed of data sent from many different host computers, each of which must be queried and respond to each data request of your browser. Each of these query and response cycles takes time, and a page which has an excessive number of these requests, such as one with several different advertisements, can slow down the loading of a web page dramatically. Not only does the downloading of the data for a single page take longer, but all those packets of unnecessary and often undesired data flying about slow the speed of the entire World Wide Web. It is as if we have taken the now heavily traveled "information superhighway" and populated it with empty cars.

When @Guard blocks these things, what it's doing is blocking the outbound request that the browser makes for the image. The blocked data IS NEVER TRANSFERRED, so pages load faster and the internet has less clutter.

The example string, "http://www.foo.com/nifty_images/image7.gif", is known as a URL, or Universal Resource Locator. @Guard lets you block it if any part of it matches a string in your blocklist, so if you put either "www.foo.com", "nifty_images", "image7.gif", or something more specific like "foo.com/nifty_images/image7.gif" into the blocklist, the image would be blocked.

The particular string that you choose to block a data request (such as an advertisement) will affect how restrictive or unrestrictive @Guard will be in its filtering of data. For example, if you put simply "foo.com" into the All Sites blocklist, you would wind up blocking EVERYTHING that comes from foo.com. If you were much more specific by using "www.foo.com/nifty_images/image7.gif" to block the same thing, you would probably wind up blocking only that one particular image on one particular web page.

You can also be more specific by adding a Site entry for "foo.com" or "www.foo.com", and then adding "image7.gif" to that Site's Block String list. Strings that you add to a Site-specific blocklist WILL ONLY APPLY to tags on pages coming from that site or to outbound requests going to that site. Note that the Ad Trashcan always adds strings to a Site-specific entry in the blocklist, rather than adding strings to the All Sites list.

The Block Strings under a Site entry of "foo.com" will be used to match "www.foo.com", "stuff.foo.com", "adserv.foo.com", and so on. However, a Site entry of "www.foo.com" will NOT match "adserv.foo.com". This is an edit that I often make after I've used the Ad Trashcan: Changing a hostname like "www.foo.com" to cover the entire domain, such as "foo.com".

3-2. How do I block an image using Netscape?

First, bring up the Ad Trashcan by clicking on the @Guard icon on the right side of the taskbar and clicking on the "Ad Trashcan" menu item. You should then have a window with a trashcan in it that does not look like the desktop Recycle Bin. Then, in either Netscape 3.0 or 4.0, right-click on the image you want to block. You should see a menu with "Copy Link Location" or "Copy Image Location" or both, toward the bottom of the menu. Select one of those to copy the URL to the clipboard, and then right-click on the trashcan to paste it into the blocklist.

The trashcan looks back at the web page data it has seen recently, finds something that's a close match with what you dropped into it, and brings up a dialog box telling you what it just added to the blocklist. Depending on what it came up with, you may want to go modify the new blocklist entry. (see section 3-6)

3-3. What's the difference between "Link Location" and "Image Location"?

Some images take you to other pages when you click on them, or at least that's what appears to happen. What really happens is that your browser loads a new page that was associated (using HTML, or HyperText Markup Language) with the image you clicked on.

The URL that your browser used to fetch the image in the original page is the "Image Location", and the URL that your browser uses to fetch the new page is the "Link Location". You can block an image by adding a string that matches EITHER its Image Location OR the Link Location associated with it.

That leads to a potentially useful generalization: If you want to customize a particular page, being specific about the Image Location by using a blocklist string such as "www.foo.com/nifty_images/image7.gif" usually works well. On the opposite end of the spectrum, if you want to block all of the images that take you to a site whose only purpose is to sell you shoes for your pet wombat, it often works well to use a very general blocklist string, like "www.wombatshoes.com", or even just "wombatshoes.com".

Be careful that what you put into the blocklist isn't too general. Something like "www" is not a good blocklist string because it would match far too many URLs. (see section 3-7 for how to tell if you're missing things.)

Using the Ad Trashcan to block images is the "safe" way to go because it uses Site-specific entries. Manually adding entries to the blocklist using All Sites entries is the "power-user" way to go because it allows you to be much more general about what you're blocking (at the risk of blocking too much).

3-4. How do I block an image using Internet Explorer?

First, bring up the Ad Trashcan by clicking on the @Guard icon on the right side of the taskbar and clicking on the "Ad Trashcan" menu item. You should then have a window with a trashcan in it that does not look like the desktop Recycle Bin. Then, in either Internet Explorer 3.0 or 4.0, click and hold on the image you want to block and drag it onto the Ad Trashcan.

The trashcan looks back at the web page data it has seen recently, finds something that's a close match with what you dropped into it, and brings up a dialog box telling you what it just added to the blocklist. Depending on what it came up with, you may want to go modify the new blocklist entry. (see section 3-6)

When you drag an image into the trashcan, Internet Explorer always uses the Link Location, with one exception: When the image has no link associated with it, Explorer uses the name of the file in its disk cache, and @Guard makes the best guess it can as to what portion of the name to use. (see section 6-11) By right-clicking on the image on the web page, however, it is possible to get the Image Location from Explorer.

3-5. How do I block an image using a different browser?

If your browser allows you to right-click on an image and copy either the image location URL or the link location URL to the clipboard, you should be able to paste it onto the Ad Trashcan just as you would if you were using Netscape.

Otherwise, you may need to look at the HTML source code and find the <IMG SRC="blah/blah/image_name"> image location string and copy a piece of it to the clipboard to paste into the blocklist.

3-6. How do I modify or remove entries in the blocklist?

Go to the Settings dialog by clicking on the @Guard icon on the right side of the taskbar and clicking on the "Settings" menu item. Select the "Ad Blocker" tab (if it isn't already selected) and note the list of Sites under the URL Blocking List in the window. Now, select a Site (or All Sites) in the left hand window, and a scrollable list of strings associated with that Site appears in the right hand window. You should be able to move the elevator bar up and down to scroll through the list. When you see the string you'd like to modify or remove, click once on it to select it and then click on either the "Modify..." or "Remove..." button.

Modifying or deleting blocklist entries is sometimes required for new entries that didn't come out as you expected, or just to change what's being blocked.

3-7. How can I tell if I'm blocking too much?

@Guard logs all the things that it removes to the Ad Blocking tab of the Event Log. You can bring up the Event Log by clicking on the @Guard icon on the right side of the taskbar and clicking on the "Event Log" menu item.

If you are looking at a page and it doesn't seem quite right, you can look at the Ad Blocking tab and see the web page elements that @Guard most recently removed. Clicking on a particular line will bring up more information about it in a window at the bottom of the Event Log dialog. You should see "Removed", which is the HTML element that the browser was prevented from retrieving, "From", which is the URL of the web page you were looking at that the blocked element would have been requested from, and "Because", which is the string in the blocklist that caused the thing to be blocked.

If you see a large number of things being removed from several different "From" locations all for the same "Because" reason, it could be an indication that the "Because" string is too general, and you might consider either removing it from your blocklist or moving it from the All Sites list to a Site-specific list.

You can also go to the Settings dialog, turn off URL blocking, and reload the web page to check the differences between the page with blocking enabled and the page with blocking disabled. NOTE: Be sure to clear your browser's web page cache before doing this test, or you won't see any changes even if @Guard had been blocking a dozen images!

This makes for a good experiment: Manually add a string that is certain to match way too much, such as "/" (a slash without the quotes) to the All Sites blocklist and load a web page to see the effects.

Obviously, you'll want to remove the string right after you do this experiment, because a single forward slash will match (and therefore block) almost everything. Go to a web page, and it will probably be completely blank. Now, go look at the Event Log's Ad Blocking tab and click on the entry in the top of the list of things that were recently Removed. The "Because" line in the Event Log bottom window will probably read simply "/", which is certain to cause far more blocking than you want.

If pages start looking like the blocker is catching too much, look in the Event Log for "Because" strings that may be too generic.

3-8. What happens with animated GIFs?

Animation blocking only applies to GIFs that were not blocked in the first place. All of the frames of an animated GIF are fully downloaded, and if animation blocking is enabled, will run through a single cycle of animation and then stop.

Aside from reducing the visual distraction level of some pages, this can also dramatically reduce "disk thrashing", which occurs when the browser stores all of the animation frames in its cache and continuously re-reads them in order to display them. For laptops, that can mean increased battery life.

3-9. Why is there sometimes an empty square or rectangle on the page?

In some cases, @Guard blocks an image by replacing it with a transparent

GIF. If the unblocked GIF would have had a border around it, the transparent GIF gets one also. In those cases, the link is usually still present, meaning that it's possible to click on the empty area and go to the web page associated with the blocked image request.

3-10. What's the diff between All Sites and a Site-specific blocklist?

Strings that are added to the All Sites list (@Guard comes with about 50 strings in that list by default) are used to remove images from any page you visit. The All Sites list is also the place to add entire domain names that you want to block. A Site-specific list is used when you want to add a Block String that will only be used when processing HTML coming from that Site or when blocking images from that Site.

----- 4. PRIVACY: COOKIES AND REFER FIELDS -----

4-1. What are cookies?

Cookies are bits of information that web servers store on your computer for their own later use. Web servers can use cookies to keep track of how many times you've visited and when, what sort of info you've been surfing for on their site, and even use them to pass that information on to other web servers, such as advertisement servers.

On the positive side, cookies can be used to store your own web site configuration, to remember items placed in your "shopping cart" at an on-line shopping site, or to store account and password information for subscription sites. You may want to allow cookies on certain sites, hence @Guard's cookie Site and Domain list.

4-2. Why does my browser keep warning me about accepting cookies?

You've probably got your browser configured to warn you before accepting a cookie. Since AtGuard prevents cookies from being sent to web servers, (and logs what it blocked and what it allowed), it's safe to change your browser to go ahead and accept cookies without bugging you.

To verify that cookies are in fact being blocked, make sure that "Enable Cookie Rules" is checked and the "Block cookies without rules" radio button is selected in the Privacy dialog of Settings. Do some surfing, and you should see the "Cookies Blocked" counts going up in the Statistics window. You should also see what action was taken with the cookies in the Event Log under the Privacy tab.

4-3. How does @Guard block cookies?

Cookies are blocked on the way OUT of your computer, NOT on the way in. Incoming cookies are accepted, but the information that they contain is not allowed to be sent back to a web server unless you explicitly put the domain name of the server into the cookie allow list.

A number of cookie-blockers work this way, probably because it's easier to implement. There are several ways for web servers to set cookies on your computer, but there's only one way that browsers give cookies back to web servers. If they're blocked on the way out, the blocker catches all of them.

4-4. How do I block some cookies but not others?

With "Enable cookie rules" checked and "Enable CookieAssistant" selected, any outbound cookie for a Site/Domain that is not in the Privacy window's Site/Domain list will cause a dialog box to pop up and ask you what you want to do with the cookie. The CookieAssistant dialog allows you to create a rule right then and there. If it's a page you visit often and you use features of it that require cookies, you'll probably want to Permit cookies for that domain.

The CookieAssistant method is the easiest way to create cookie rules. However, running with it turned on all the time tends to lead to a large list of Block rules. I tend to hit the "Always block" button in the CookieAssistant dialog about 99.9% of the time. I'm sure not going to allow a cookie when visiting a strange site. So, rather than be bothered with CookieAssistant dialogs, I turn on the CookieAssistant only when I want to create a Permit rule for a Site. The rest of the time, I run with "Block cookies without rules" turned on. I wind up with a very small set of Permit rules rather than a large set of Block rules.

Power users can go to the Privacy tab of the Settings dialog and manually add the domain name for a site to which to allow cookies to be sent, and "Permit" for the Action to take.

The name you want is usually the same name as the site you're visiting, but an easy way to check is to bring up the Privacy tab in the Event Log and then go visit the web site that is setting the cookies you want to permit. After the web page is done painting, hit the Refresh button on the Event Log and you should see something like this:

```
Blocked Cookie: WPI=890793854.jw.00132 sent for http://www.javaworld.com/
```

The thing on the left of the "sent for" is the value of the cookie, and the thing on the right of the "sent for" is the thing that was being requested. This cookie was being sent to www.javaworld.com, so I can add "javaworld.com" (without the quotes) to the cookie list.

You can copy selected text out of the lower window in the Event Log by selecting it with the mouse and hitting ctrl-C. Then, when you hit the "Add" button in the Privacy tab of the Settings dialog, you can hit ctrl-V to paste it in.

With "javaworld.com" in my cookie list with Permit as the action, I see the following when I visit javaworld:

```
Allowed Cookie: WPI=890793854.jw.00132 sent to http://www.javaworld.com/
```

4-5. What are "referer fields"?

When you click on a link to a web page, your browser makes a quick note of what page you are currently viewing. When it sends the request for the new page, it passes that information on to the new server. That allows web servers that you visit to know where you've just been, which is information that you might prefer to keep to yourself.

When refer fields are allowed, your browser tells a web server that you are visiting that you clicked on a link to get to them. It also tells them what page it was that you were just visiting! When refer fields are blocked, however, the web server that you are getting a page from thinks that you just typed the URL into your browser or selected it from your bookmarks.

Cool trick: Bring up the Privacy tab in the Settings dialog and right-click on "Block refer fields". You'll get a better explanation of what the "Block refer fields" checkbox does than what I've got here. You can right-click on a bunch of things around the Settings dialog for more info.

4-6. Why aren't a lot more refer fields being logged?

Refer fields are also sent by the browser for every separate piece of a web page that's downloaded, so astute observers will notice that only a fraction of all the actual refer fields that are sent are being logged. What's happening is that @Guard only concerns itself with refer fields when your browser is telling a host that it was referred by a different host.

If you visit www.yahoo.com and the opening page tells the browser to retrieve one image from yahoo.com and one image from advertisers.com, @Guard will always let the refer field to yahoo.com through because it's going to the same host that the referring page was obtained from, but will block refer fields to advertisers.com because the request is going to a different host. The reason for this is because some web sites use refer fields to prevent other web sites from linking into the middle of their pages. Also, because a host knows that you just visited it, there's little privacy to be gained by blocking a refer field that's going back to a host you just visited.

4-7. Why is "referer" misspelled?

HTTP legacy is behind this. Inside the actual HTTP header that the browser sends to a web server when you click on a link is the referrer field, spelled "Referer:". Long ago, some programmer who couldn't spell referrer came up with that field name. Hundreds of thousands of installed web servers, all looking for a field called "Referer:", makes it quite difficult to correct the spelling within the HTTP header. It's rarely seen by humans though, so it doesn't really matter.

----- 5. FIREWALLS AND SAFETY -----

5-1. How do I enable the @Guard Firewall?

The @Guard Firewall can be turned on (it is off by default) by going into @Guard settings (see section 2-6) and going into the Firewall tab. Then, click on the Enable Firewall checkbox.

5-2. What does the @Guard Firewall do?

The @Guard Firewall, when enabled, intercepts both inbound and outbound connection attempts and packets on your computer and decides whether to allow or deny them based on a list of rules that you define. If the "RuleAssistant" (interactive learning mode) is enabled and @Guard sees a connection attempt or packet that it has no rule for, it puts up a dialog box to tell you what's happening and ask you how to deal with it now and in the future. With the RuleAssistant feature, it constructs firewall rules on the fly.

@Guard can protect against data being transmitted without your knowledge. It can warn you about attempts to use resources on your computer that you might otherwise not know about, help you learn about the resources your computer makes available to others on the internet, and provide you with a way to control who connects to your computer and who your computer can connect to.

5-3. How does the firewall block connections?

The firewall consults a list of rules, visible in the Firewall tab of the Settings dialog, when it needs to decide how to deal with a connection. When a new connection or packet needs to be dealt with, the firewall goes down the list of rules, IN ORDER, looking for the first rule that matches the connection or packet type in question. If no match is found, the connection or packet is denied. However, if the RuleAssistant is enabled, an alert pops up and will give you several options on how to deal with this communications attempt.

5-4. Why are RuleAssistant alerts popping up?

You've got the @Guard Firewall and RuleAssistant enabled, and something is trying to communicate to or from your computer. The RuleAssistant will indicate several things to you:

- If your computer is establishing communications to a remote computer (outbound) or if some remote computer is establishing communications to your computer (inbound).
- The inbound or outbound service name or port number
- The name of the application on your computer that is responsible for the communications attempt

The most common reason for an alert to pop up is that you ran an application that is trying to establish an outbound connection with another computer. (The RuleAssistant will always indicate to you what application is making the attempt.) In this case, you probably want to allow it, and you might even want to create a rule to allow it in the future so that you aren't warned every time you try to use that application. In this case, once you have RuleAssistant create a rule to always permit this application, you are now giving this application a green light to establish any communications. Consider it now to be a trusted application.

If, on the other hand, the application is something that you think shouldn't be communicating with other computer, such as a newly installed text editor or a paint program you downloaded from the Internet, you may want to create a rule to block communications for that application.

If the communication was inbound, again, RuleAssistant will indicate to you what application is responsible for the communcations attempt. Before you get too suspicious of remote computers trying to connect to yours, bear in mind that programs often create more than one connection, and some client programs that you run communicate with remote servers by asking them to connect back into your computer. An FTP client is a good example of this; when you run an FTP client to connect to an FTP server, one alert usually pops up to tell you about an outbound connection, not surprisingly. Then, more alerts come up to tell you about the remote FTP server connecting back to your FTP client whenever you send a command to the FTP server to do something.

5-5. What should I do when a RuleAssistant alert pops up?

The first thing to do is try to understand what communication happened that made it pop up. Then, you need to decide whether to permit or block the communication. Finally, you need to decide whether to have RuleAssistant create a rule for you that @Guard can apply for future communications attempts.

The Application name shown in the alert dialog is usually enough to give you an idea of what happened, especially when the communication is coming from a program that you just ran. The alert dialog also gives you the "service" or port number to consider, and the address or name of the remote host computer as well.

If you're just starting out, it doesn't hurt to try blocking or permitting the connection for "just this attempt" until you get a feel for how often the communication occurs. You can also check the Event Log's System tab to see events logged by the firewall, including how rules are being processed and any connections that were blocked. The Connections tab shows information about successful connections, whether permitted by the firewall or because the firewall was not enabled.

5-6. What does "Always permit in/outbound communication for this app" do?

When you choose that option from the RuleAssistant alert, a PERMIT rule is created for a particular application, giving it permission to establish connections to any host using any port number that it pleases.

After creating a rule, it is possible to go back and make changes to it to make it more or less restrictive. After initially granting permission to your email client to connect to your Internet Service Provider's mail server for example, you may wish to edit the rule to restrict your email client's connections ONLY to your ISP's mail server.

5-7. How about "Always permit in/outbound communication for this service"?

When you choose that option from the RuleAssistant alert, a PERMIT rule is created to always permit communications to or from the indicated service (port number).

Say, for example, you ran an FTP client to transfer a file from an FTP server on the Internet. You would first get an alert warning you that your FTP client was trying to make an outbound connection to the FTP server. If you choose to always permit outbound connections for the ftp service, then the rule will permit ANY FTP client application on your computer to establish a connection to a remote host without alerting you.

5-8. What does "Always block this in/outbound network communication" do?

When you choose that option from the RuleAssistant alert, a BLOCK rule is created that's very specific about what it's blocking. The rule includes the application name, the particular service (port number) that an attempt was being made to communicate on, and the address of the remote system.

Once you create a block rule, you can always change your mind and edit the rule that was created at a later point in time. Sometimes, after creating a rule, you may want to be more or less specific. For example, you may have had the RuleAssistant create a rule to block a connection attempt to a certain remote machine. You later decide you want to edit the rule to be more general to block this same communication to other remote machines that are perhaps on the same network as the original one you blocked. By editing the rule, you can change it to specify more than one remote address by specifying a remote network address, rather than just a single remote host address that was originally created.

5-9. What are services? What are port numbers?

Many host computers that are connected to the Internet offer services, such as HTTP servers (HyperText Transfer Protocol to provide World Wide Web service), FTP servers (File Transfer Protocol), SMTP servers (Simple Mail Transport Protocol to provide mail sending), and POP servers (Post Office Protocol to provide mail retrieval). Services are protocols that are used to allow one computer to access a particular kind of data stored in another computer.

A computer that is connected to the Internet is usually assigned a 4-byte Internet Protocol address (an IP address) that is used to distinguish it from all other computers connected to the Internet. When you connect to a web server, for example, you may tell your browser to connect to www.technologypreview.com, but your computer ultimately has to translate the name to its IP address, 199.238.200.110, before the connection can be made.

When the connection is made, we also need a way to tell the computer that we're connecting to which of its services we're interested in. The host computer may be running both an HTTP server and an FTP server, and if we're connecting to the host computer using a web browser for example, we'll want to connect to the HTTP server and not the FTP server. This is done using port numbers. Since HTTP servers usually listen on port number 80, and FTP servers usually listen on port number 21, our web browser will connect to the correct server on the www.technologypreview.com computer if it connects to port 80 of the computer at 199.238.200.110 rather than to port 21. Port numbers are arbitrarily-chosen numbers associated with particular services, and are always used in conjunction with IP addresses when establishing connections to host computers.

This section is quite a brain-filler, but once you've got it, you've got the basis by which all kinds of different data flies around on the Internet! Search for a file called "services" on your computer for an interesting list of some of the different kinds of services and what their "standard" port numbers are. If you're like me, it'll keep you spellbound for hours on end.

5-10. What's the diff between TCP connection attempts and UDP packets?

A connection attempt is really just a TCP packet that is asking to establish a connection to or from your computer that may last anywhere from milliseconds to hours. A UDP packet, on the other hand, is a single packet used to transmit information without the implied promise of any additional information being transmitted. Your computer can send or receive a single UDP packet to exchange information without any connections being established.

An example of both kinds being used occurs when you use a web browser to download a web page. If you go to http://www.technologypreview.com, for example, your computer first sends a UDP packet out into the world to try to find out what the 4-byte Internet Protocol address is for the computer called "www.technologypreview.com". The protocol used to do that is called DNS, or Domain Name Service, and the queries and replies take place without any persistant TCP connections being made. Having a rule to allow this to happen is important (that's mostly what those predefined Inbound UDP and Outbound UDP rules are for) or your computer wouldn't be able to talk to other machines at all. UDP, or connectionless communication works well for DNS because the queries and replies are very small and can be completed in single packets. Once we've got the 4-byte IP address for www.technologypreview.com, however, we need to establish a persistant connection with it in order to fetch the web page and images because there's more data to be moved than will fit in a single packet. That's where TCP connections come into play; a TCP "SYN" (synchronize a connection) packet is sent to the web server, it replies with a TCP "ACK" (acknowledgement), and voila, a connection is created between the two computers and the data starts to flow.

By default, when the @Guard Firewall is enabled, inbound and outbound UDP packets are permitted. This can always be changed by editing one of the @Guard Firewall rules.

5-11. Why is there sometimes no alert when someone tries to connect to me?

If you are not running a program on your computer such as an FTP server, finger server, telnet, or web server, then the TCP/IP network software below @Guard knows that no software is listening on the port that the connection attempt was made on, and it will reject the connection without any notification making it up to @Guard. For inbound TCP connections, @Guard only alerts you when your computer is running a server program that could be connected to (and if there's no rule for the operation defined).

THIS SECTION UNDER HEAVY CONSTRUCTION

5-x. Can I use 4-byte IP addresses in place of address names in rules?

5-8. Can I fine-tune rules that were created using the RuleAssistant?

Yes. Say for example that you had created a rule to allow any outbound connections on the ftp port, but you'd like to be alerted to any attempts to establish FTP connections by programs other than your trusted FTP client.

5-x. How do I create firewall rules manually?

5-x. What are the specific things that can be defined in a rule?

5-x. Help! What is all this gibberish about services, ports, TCP, etc?!?

Hang in there! You probably need some more basic information about how host computers and your computer communicate with each other over the Internet before firewalls start making sense.

Don't be afraid to experiment with the firewall, to enable it and try making connections to see what it detects and how it responds. The @Guard firewall is actually a pretty good way for newcomers to networking to get a feel for how programs talk to each other.

About the only thing to watch for is not to delete the four default rules for Inbound UDP, Outbound UDP, Inbound TCP loopback, and Outbound TCP loopback. If those rules get deleted, your computer probably won't be able to do much if the firewall is enabled.

5-x. Help! I removed all of the Firewall Rules, and now I'm stuck!

For a quick fix, just disable the firewall. For your computer to do much of anything with the firewall enabled, you'll want to have at least four rules in the Firewall Rule list. They're pretty easy to create:

Rule 1: Inbound UDP
Rule 2: Outbound UDP
Rule 3: Inbound TCP loopback
Rule 4: Outbound TCP loopback

----- 6. OTHER STUFF -----

6-1. When I turn @Guard <off/on> and reload the page, it still <is/isn't> blocking images!

A common problem is that the reloaded page is coming from your browser's local history of web pages (the cache) and not from the actual server. You need to clear your web browser's cache.

6-2. What is the web browser's cache?

Because transferring web pages over the internet from a web server to your computer takes time, the people who write browsers came up with a nifty trick to speed up the displaying of pages. Before your browser sends a request to a web server for a page, it first checks to see if it has seen that same web page recently. This occurs more often than you might think, such as when you hit the Back button in Netscape or Explorer.

If the web page is in your browser's list of recently-visited pages, called the cache, then it is read right from your hard disk. This is much faster than retrieving it from the web server.

However, reading the web page from your hard disk also bypasses your computer's network software, which also means that @Guard will not see any requests going to web servers and won't have anything to block. If the web page in the browser's cache is full of images you want to block, you'll need to clear the cache before @Guard can block them. The reverse can also be true: If the web page in your cache has already had images blocked and you want to disable blocking, you'll need to clear the cache or your browser won't realize that there are now "new" images to be retrieved.

6-3. Anything I should watch for when installing on a dual-boot machine?

Yes. The most important thing is not to install to the same directory. On Win95, I installed @Guard in c:\block95 and on NT I installed in c:\blocknt.
You can install it wherever you like, but you'll definitely want to use different directories. This is usually a good rule of thumb for most Win32 software installed on a dual-boot machine.

6-4. How do I find the version number?

Go to the Settings dialog (see section 2-6) and click on the "About" tab. You'll also see versions and sizes for various DLLs that @Guard has loaded.

6-5. Why do some pages come up completely blank?

There is probably a string in your blocklist that is too generic and is matching more than you want. If a page loads and it's totally blank, go to the Event Log and check to see what the last blocklist string was (in the "Because" field) that blocked something. Chances are that removing that string from the blocklist will clear up the problem.

Another cause is what appears to be a bug in Netscape. Sometimes, Netscape simply fails to paint after retrieving a page. I've seen this happen in Netscape 3.0 on Win 3.11, Win95, and WinNT, and 4.0 on Win95 and NT without any other 3rd party software installed. Tread lightly, 'cause it sometimes page faults soon after.

6-6. An image STILL isn't being blocked. How do I block it?

In order for a browser to display an image, it needs to request that image from a web server. If the actual Image Location URL is in the blocklist (as opposed to the Link Location URL, where you'd be taken to if you clicked on the image), the image request will be blocked by @Guard. So for tough stains, er, images, we need to make sure we've got the Image Location URL in the blocklist, and not the Link Location.

This can be easier said than done. Internet Explorer 4.0, unfortunately, likes to give Link Locations instead of Image Locations when images are dropped into the Ad Trashcan. If the link location is something "unsafe" to add to the blocklist (such as "/" or "/index.html") the Trashcan will offer to add the full URL to the blocklist, which won't block the image. With Explorer 4.0, it's often necessary to get the Image Location by right-clicking on the image, selecting "Properties", and copying the Image Location URL off of the dialog. Then, you can right-click on the Trashcan and paste the URL into the blocklist.

Image maps are difficult to determine the Image Location for because a single image can have multiple Link Locations, and Explorer picks whichever one the mouse is on when it is dragged. With an image map, the only way to block it is to use the Image Location URL.

6-7. How do I find the Image Location URL for a particular image?

In Netscape, right-clicking on the image and copying its Image Location to the clipboard, then pasting the location into Notepad or into the browser's Location or URL entry field usually works.

In Explorer, right-clicking on the image and selecting Properties displays a dialog that contains the Image Location.

In the worst case, it may be necessary to look at the HTML source and try to find the SRC="... statement associated with the image. This isn't always as bad as it sounds, especially when the image is close to the top of the page or there aren't too many images on the page. It helps to get the image properties before looking at the HTML source

If you pulled up the image properties and have a string to search for, Explorer's View Source window (Go to the View menu, then select Source) allows you to search for a string in the HTML source. Netscape's View Source window (Go to the View menu and select Document Source or Page Source) does not, so you'll have to select all (ctrl-A), copy it to the clipboard (ctrl-C), paste it into your favorite text editor and search for the string there.

If the page is relatively small, you can do an eyeball-search for "<img" tags to find the image references on the page.

Link Location strings are often of the form:

```
<A HREF="http://www.foobar.com/dir/path/webpage.html">
```

and Image Location strings usually look something like:

```
<IMG SRC="path/path/path/filename.gif">
```

Also, they are almost always close to each other, with the Link Location coming right before the Image Location. Here's an example taken from WRQ's Technology Preview page at http://www.technologypreview.com

```
<tr><td valign=top align=center><a href="http://www.wrq.com">
<IMG SRC="images/buttons/k_wrqhome_up.gif" WIDTH="95" HEIGHT="22" Border="0">
</a></td></tr>
```

Note that the HTML commands like HREF and SRC are not case-sensitive.

6-8. Any undocumented registry entries?

First off, don't mess with the registry unless you know what you're doing and you've done it before. I think I know I'm doing, but I'm obviously mistaken since I've hammered my machine several times while twiddling the registry and had to erase my disk and do a clean install in order to recover. So, since you're not going to mess with the registry anyway, here are a couple tidbits:

@Guard stores its configuration info in HKEY_LOCAL_MACHINE->SOFTWARE->WRQ->IAM in a number of subkeys, including:

```
HTTP Performance
  FilterEnable   00 or 01
    This is used to globally turn the HTML filter on and off, although
    no checkbox exists anymore in the UI for it.
  FilterText     00 or 01
    When set to 01, an anchor tag that has no IMG SRC= part to it gets
    wiped out if the HREF part matches something in the blocklist.
    With FilterText turned on, you can actually block text-only links.
```

6-9. Why doesn't the statistics window show a count of bytes rejected?

That would be great info to have, but unfortunately, there's no way to know how many bytes have not been received when an image is blocked. @Guard didn't receive the data, so it couldn't count them.

6-10. Is the Ad Trashcan editing URLs that are dropped in it?

Yes. If you have a string to add to the blocklist manually, it's best to go add it directly to the blocklist via the Settings dialog.

When a URL is dropped into the Ad Trashcan, the trashcan looks back in a list of HTML string fragments that it saw when you loaded a recent page. It tries to find a match so that it doesn't add the entire string to the blocklist. In many cases, adding to the blocklist the full URL string that the browser gives you when you copy the Image or Link Location or drag the image won't work because the full URL doesn't necessarily appear in the HTML.

For example, the actual HTML might read <IMG SRC="huge_images/ad9000.gif">, while the browser gives you the full URL, which might be "http://bandwidth.eater.com/huge_images/ad9000.gif". The Ad Trashcan would try to reduce the full URL down to "huge_images/ad9000.gif" if it can.

6-11. Does @Guard keep any of its files in the windows system directory?

Yes. They all begin with "iam", so they're easy to find if need be. For Win32 programs, there's occasionally a choice between having to have DLLs in the path or in the windows system directory. @Guard chose not to require an entry in the path.

6-12. Netscape hangs when...

Yes, that happens to me often on Win 3.1, Win95, and WinNT. If you're getting weird hang behaviour with Netscape, try to duplicate it using Explorer before pointing the finger at installed network filters, service providers, the version of the Winsock DLLs, network load, ambient temperature, phase of moon, etc.

My current theory is that Netscape doesn't always seem to recover from network connections that aren't completed in a timely fashion, so if the network is slow or packets are being lost in the net when downloading web pages, Netscape is more likely to hang. Hitting the Stop or Cancel button while downloading a page, or clicking on a link before a page is completed seems to help it demonstrate hangness. Your mileage may vary.

6-13. Does @Guard slow down my browser?

The filtering that @Guard does shouldn't slow network packet processing down by much at all. The work that @Guard has to do to watch network connections and parse HTTP data within your computer is negligable compared to the time it takes for data to travel from one computer on the internet to another. The processing that happens within a packet filter in a PC is typically measured in microseconds, but the time it takes for packets to move around on the net is measured in milliseconds. For handling big blocklists, @Guard uses a very cool algorithm/data structure combo called an Aho-Corasick character tree that allows for some very fast searching. (There's an article in a 1970 issue of CACM that describes the Aho-Corasick algorithm for any propellorheads out there.)

@Guard does confuse some performance monitor programs. When sitting idle and doing nothing, @Guard blocks in a system driver. This cause some really lame performance monitors to report %100 CPU utilization, when it's obvious that there's plenty of CPU left. I understand that WRQ is tweaking @Guard to use a method that the Microsoft and Norton performance monitors can understand to cut down on the number of people asking why their performance monitor shows 100% CPU usage, but the method is actually LESS efficient than just blocking. Bummahz.

6-14. Why can't I exit @Guard like I exit other programs?

@Guard installs itself at boot time as an NT kernel driver or a Win 95 VxD. It does this before any applications run, which makes it very hard for applications to circumvent it. This is especially important for the firewall. A side effect of being a kernel driver this is that it is not easy to remove @Guard or re-run it without rebooting the computer. This shouldn't be a problem since @Guard doesn't actually do anything until it has to handle some network traffic. Leaving it in memory shouldn't do much except consume a little memory.

Like other system device drivers, it's not a program that you start when you want to use it and exit when you're done. The equivalent of "exit" for a Windows system device driver is to uninstall and reboot. In addition to the network device driver, it does use a process called Iamapp and a service called Iamserv to handle things like event logging and the user interface. A feature to start and stop those processes might be added at some point.